IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Antony John Rogers, et al.

Serial No.:   09/905,532

Filing Date   July 14, 2001

Group Art Unit: 2437

Confirmation No.:   3485

Examiner: Michael J. Pyzocha

Title: *DETECTION OF VIRAL CODE USING EMULATION*
                             OF OPERATING SYSTEM FUNCTIONS

MAIL STOP AF
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to OG Notice, this Request is being filed concurrently with a Notice of Appeal. Applicants respectfully request reconsideration of the Application in light of the remarks set forth below.

The Office Action issued October 22, 2008 (the "Office Action") rejected Claims 1, 4, 8-16, 20, 22 and 23 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,192,512 issued to Chess ("*Chess*") in view of U.S. Patent No. 5,851,057 issued to Nachenberg ("*Nachenberg*") and the Final Office Action issued February 10, 2009 maintained these rejections. The rejections include clear legal and/or factual errors, however, and Applicants respectfully traverse the rejections.

First, the proposed *Chess-Nachenberg* combination fails to disclose "in response to detecting an attempt to access the artificial memory region, determining an export table entry in the export table of the dynamically-linked library that is associated with the attempt to access the artificial memory region" as recited by Claim 1. As Applicants previously noted (*see, e.g.,* Response to Office Action filed January 22, 2009 (the "Previous Response") at pp. 11-12), the Office Action failed to address the language of this element entirely. In response to this argument, the Final Office Action belatedly attempts to remedy this deficiency by making several inaccurate assertions about what the references teach. For example, according to the Examiner, "*Nachenberg* teaches monitoring entry points of viruses by emulating the applications, determining where virtual memory has been modified and reporting which entry point is infected." Final Office Action at p. 6. Applicants respectfully note that this assertion inaccurately paraphrases the cited portion of *Nachenberg*. The cited portion states instead that "the VDS (400) uses the scanning module (424) to *scan pages of the virtual memory (434) that were either modified or emulated through* for signatures of polymorphic viruses and uses stochastic information obtained during the emulation, such as instruction usage profiles, to detect metamorphic viruses. If the scanning module (424) or VDS (400) detects a virus, *the VDS reports that the file (100) is infected.*" *Nachenberg* at col. 4, ll. 59-64, emphasis added. The cited portion does not indicate that the system of *Nachenberg* "determin[es] *where* virtual memory has been modified" (emphasis added) or that it "report[s] *which entry point is infected*" (emphasis added) as the Examiner contends. Thus, the rejection of Claim 1 relies on an improper paraphrasing of the cited reference, and the rejection therefore includes clear factual and/or legal errors.

Additionally, the proposed *Chess-Nachenberg* combination also fails to disclose "determining based on the export table entry associated with the attempt to access the artificial memory region that the emulated computer executable code is viral" as recited by Claim 1. As Applicants previously noted (*see, e.g.,* Previous Response at p. 12), the Office Action failed to address the language of this element, instead addressing a paraphrased version of the claim language. In response to this argument, the Final Office Action belatedly attempts to remedy this deficiency by making additional inaccurate assertions about what the references teach and again ignoring the actual wording of the claim. The Final Office Action asserts that *Nachenberg* teaches determining that a file is viral based on accesses and/or modifications to artificial memory. Final Office Action at p. 7. As noted above, however, the cited portion states instead that "the VDS (400) uses the scanning module (424) to **scan pages** of the virtual memory (434) that were either modified or emulated through **for signatures of polymorphic viruses and** uses stochastic information obtained during the emulation, such as instruction usage profiles, **to detect metamorphic viruses**. If the scanning module (424) or VDS (400) detects a virus, the VDS reports **that the file (100) is infected.**" *Nachenberg* at col. 4, ll. 59-64, emphasis added, not that the system "teaches determining that a file is viral based on accesses and/or modifications to artificial memory" as the Examiner asserts. Furthermore, even if the Examiner were correct, Claim 1 recites "determining **based on the export table entry associated with the attempt to access** the artificial memory region that the emulated computer executable code is viral" (emphasis added), which the Examiner does not even attempt to argue is disclosed by the proposed combination. As a result, the proposed combination also fails to disclose this element of Claim 1, and the rejection of Claim 1 includes clear legal and/or factual errors for at least this additional reason.

Although of differing scope from Claim 1, Claims 10-12 and 14 include elements that, for reasons substantially similar to those discussed with respect to Claim 1, are not disclosed by the proposed *Chess-Nachenberg* combination. Claims 10-12 and 14 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 1, 10-12 and 14, and their respective dependents.

CONCLUSION

As the rejections of Claims 1, 4, 8-16, 20, 22 and 23 contain clear deficiencies, Applicants respectfully request full allowance of Claims 1, 4, 8-16, 20, 22 and 23. To the extent necessary, the Commissioner is authorized to charge any required fees or to credit any overpayments to Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Todd A. Cason
Reg. No. 54,020

2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6452

Date: July 9, 2009

CORRESPONDENCE ADDRESS:

Customer Number: **05073**